

RECEIVED
CENTRAL FAX CENTER

JAN 13 2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10013891-1IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): SPENCER, Andrew M.

Confirmation No.: 9457

Application No.: 10/689,157

Examiner: TRUONG, Thanhnga B

Filing Date: October 20, 2003

Group Art Unit: 2135

Title: REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A MASTER ENCRYPTION KEY AND
ENCRYPTION KEYSMail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on November 13, 2008.☒ The fee for filing this Appeal Brief is \$540.00 (37 CFR 41.20).☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:☐ 1st Month
\$130☐ 2nd Month
\$490☐ 3rd Month
\$1110☐ 4th Month
\$1730☐ The extension fee has already been filed in this application.☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 540 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.18 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit:

OR

☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile: January 13, 2009

Typed Name: Jane S. Kim

Signature: Jane S. Kim

Respectfully submitted,

SPENCER, Andrew M.

By Ashok K. Manava

Ashok K. Manava

Attorney/Agent for Applicant(s)

Reg No.: 45,301

Date: January 13, 2009

Telephone: (703) 652-3822

Rev 10/00 (Apr 01/02)

Total number of pages: 25

RECEIVED
CENTRAL FAX CENTER
JAN 13 2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10013891-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): SPENCER, Andrew M.

Confirmation No.: 9457

Application No.: 10/589,157

Examiner: TRUONG, Thanhnga B

Filing Date: October 20, 2003

Group Art Unit: 2135

Title: **REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A MASTER ENCRYPTION KEY AND ENCRYPTION KEYS**

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEFTransmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on November 13, 2008.☒ The fee for filing this Appeal Brief is \$540.00 (37 CFR 41.20).☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:☐ 1st Month
\$130☐ 2nd Month
\$480☐ 3rd Month
\$1110☐ 4th Month
\$1730☐ The extension fee has already been filed in this application.☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 540. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.18 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit:

OR

☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile: January 13, 2009

Typed Name: Jane S. Kim

Signature: Jane S. Kim

Respectfully submitted,

SPENCER, Andrew M.

By: Ashok K. Manava

Ashok K. Manava

Attorney/Agent for Applicant(s)

Reg No.: 45,301

Date: January 13, 2009

Telephone: (703) 652-3822

Rev 1008(Apr09a)

Total number of pages: 26

**RECEIVED
CENTRAL FAX CENTER****JAN 13 2009****HEWLETT-PACKARD COMPANY**
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 10013891-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): SPENCER, Andrew M. **Confirmation No.:** 9457
Serial No.: 10/689,157 **Examiner:** TRUONG, Thanhnga B
Filed: October 20, 2003 **Group Art Unit:** 2135
Title: REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A
MASTER ENCRYPTION KEY AND ENCRYPTION KEYS

MAIL STOP APPEAL BRIEF - PATENTSCommissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450**APPEAL BRIEF - PATENTS**

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office Action mailed June 13, 2008, and in connection with the Notice of Appeal filed on November 13, 2008. It is respectfully submitted that the present application has been more than twice rejected. Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

01/14/2009 JVONG1 00000003 002025 10689157
01 FC:1402 540.00 DA

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

TABLE OF CONTENTS

(1)	Real Party in Interest	3
(2)	Related Appeals And Interferences	3
(3)	Status of Claims	3
(4)	Status of Amendments.....	3
(5)	Summary of Claimed Subject Matter	4
(6)	Grounds of Rejection to be Reviewed on Appeal	5
(7)	Arguments	7
A.	The rejection of claim 27 under 35 U.S.C. §102(e) as being unpatentable over Mihm should be reversed for failure to teach all the claimed features.....	7
B.	The rejection of claims 1-15 and 28-30 under 35 U.S.C. §103(a) as being unpatentable over Mihm in view of Fujita should be reversed for failure to teach or suggest all the claimed features.....	10
(8)	Conclusion	14
(9)	Claim Appendix	15
(10)	Evidence Appendix	22
(11)	Related Proceedings Appendix.....	23

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

(1) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The Appellant is unaware of any appeals or interferences related to this case.

(3) Status of Claims

Claims 1-30 are pending in the present application of which claims 1, 16, 27 and 28 are independent. Claims 16-26 are withdrawn. Claims 1-15 and 27-30 are all rejected and are all hereby appealed.

(4) Status of Amendments

An amendment after final was filed on September 15, 2008 subsequent to the Final Office Action dated June 13, 2008. An advisory action was mailed on October 1, 2008 indicating that the request for reconsideration does not place the application in condition for allowance. It appears the Examiner believes the amendment after final was a request for reconsideration even though the amendment after final included amendments to claims 27, 28, and 30. The advisory action failed to indicate whether the amendments filed in the amendment after final filed were entered or not entered. It is assumed the amendments were not entered because the Examiner indicated the request for reconsideration does not place the application in

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

condition for allowance. Accordingly, the claims presented for appeal are the claims in the response filed February 21, 2008.

(5) Summary of Claimed Subject Matter

Support for the following claims is at least provided in the cited sections of the application.

1. A removable information storage device suitable for use with a host, comprising:

a non-volatile memory configured to store a master encryption key; and See page 4, line 6-page 6, line 18 and figure 1.

a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys. See page 4, line 6-page 6, line 18 and figure 1.

27. (Original) A method of encrypting encryption keys using a master encryption key in an information storage device, comprising:

providing the encryption keys to the information storage device; See page 21, lines 1-28, and figure 12.

reading a master encryption key from a non-volatile memory; See page 21, lines 1-28, and figure 12.

encrypting each one of the encryption keys using the master encryption key; and See page 21, lines 1-28, and figure 12.

writing the encrypted encryption keys to a random access memory. See page 21, lines 1-

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

28, and figure 12.

28. (Original) A method of decrypting encryption keys in an information storage device, comprising:

reading the encrypted encryption keys from a magnetic random access memory; See page 21, line 29-page 22, line 30, and figure 13.

reading a master encryption key from a first non-volatile memory; and See page 21, line 29-page 22, line 30, and figure 13.

decrypting each one of the encryption keys using the master encryption key. See page 21, line 29-page 22, line 30, and figure 13.

30. (Original) The method of claim 28, comprising:

encrypting data using the encryption keys; and See page 21, lines 1-28, and figure 12.

writing the encrypted data to the magnetic random access memory. See page 21, lines 1-28, and figure 12.

(6) Grounds of Rejection to be Reviewed on Appeal

A. Claim 27 is rejected under 35 U.S.C. §102(e) as being unpatentable over Mihm et al. (US 2003/0236983 A1), referred to as Mihm.

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

B. Claims 1-15 and 28-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Mihm, and further in view of Fujita (US 6,947,318 B1).

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

(7) Arguments**A. The rejection of claim 27 under 35 U.S.C. §102(e) as being unpatentable over Mihm should be reversed for failure to teach all the claimed features.**

The test for determining if a reference anticipates a claim, for purposes of a rejection under 35 U.S.C. § 102, is whether the reference discloses all the elements of the claimed combination, or the mechanical equivalents thereof functioning in substantially the same way to produce substantially the same results. As noted by the Court of Appeals for the Federal Circuit in *Lindemann Maschinenfabrick GmbH v. American Hoist and Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984), in evaluating the sufficiency of an anticipation rejection under 35 U.S.C. § 102, the Court stated:

Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim.

Therefore, if the cited reference does not disclose each and every element of the claimed invention, then the cited reference fails to anticipate the claimed invention and, thus, the claimed invention is distinguishable over the cited reference.

Claim 27 recites,

encrypting each one of the encryption keys using the master encryption key; and
writing the encrypted encryption keys to a random access memory.

Mihm fails to teach encrypting each one of the encryption keys provided to the information storage device using the master encryption key. On page 3 of the Final Office Action, the Examiner asserts that paragraph 34 of Mihm discloses the EUID 162, which is stored

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

in the rewriteable nonvolatile memory 160, is formed by encrypting the UTD 152 with a master encryption key. Thus, the Examiner is asserting the master key of Mihm is the claimed master encryption key for encrypting keys provided to the information storage device. Below, a discussion of the master key and authentication process of Mihm is provided, and then an explanation follows of why the master key of Mihm is not used to encrypt keys based on the disclosure of Mihm.

Paragraphs 47 and 59 of Mihm disclose that a master key 612 is only stored in a single location and controlled by the service provider, and never requiring transmitting the master key. Thus, the master key is not stored or transmitted to the device 100. Mihm also discloses, at the service provider, the master key is used to encrypt the UID 152 to create the encrypted unique ID (EUID 614).

Paragraph 47 further discloses the EUID 614 is sent from the service provider to the device 100 as a combination 610 of the EUID 614 and the password 410. Paragraph 48 of Mihm discloses the device 100 receives the combination 610, and decrypts the password in the combination 610 using the third key 312. The decrypted password is compared to a password previously generated on the device 100. If the passwords match, the EUID 614 is stored in NVM in the device 100. This process is further shown in figures 6 and 7 of Minh.

Paragraph 48 of Mihm further discloses that after storing the EUID in NVM, the device 100 is ready to receive encrypted downloads from the service provider or perform other secure communications. This is further elaborated on in paragraph 47, which discloses the service provider receives the EUID from the device 100 when service is requested, and the service

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

provider decrypts the EUID using the master key to recover the UID for authentication purposes when the service is requested from the device 100. The authentication and secure communication is further described in paragraph 58 and shown in figures 15, 16, 20 and 21. The UID recovered from the EUID received from the device 100 at the service provider is used to generate the transport key. Also, at the device 100, the UID previously stored in the ROM is used to generate the transport key. The transport key is used for the secure communication between the device/subscriber and the service provider. See paragraph 58 of Minh.

In summary, the disclosure of Minh described above discloses the master key is used to encrypt the UID at the service provider, and the encrypted UID (EUID) is sent to the device for storage. The EUID is later used for secure communications between the device and the service provider as follows: the device sends the EUID back to the service provider; the service provider decrypts the EUID using the master key to recover the UID and generate the transport key; and the device, which previously stored the UID, also uses the UID to generate the transport key for secure communications with the service provider. Thus, the master key of Minh is not used to encrypt each one of keys provided to information storage, and then write the encrypted keys to RAM. Instead, the master key is only used to encrypt a UID. The UID is a unique identifier of a device, and not a key. Thus, Minh fails to teach encrypting each one of multiple encryption keys using a master encryption key.

The secure communications of Minh uses a transport key generated by the device and the service provider. However, Minh fails to teach the transport key is used to encrypt keys.

Instead, paragraph 58 of Minh discloses the transport key is used to encrypt software SWR_DL

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

for securely transmitting the software between the service provider and the device. Furthermore, there would be no need to encrypt keys using the transport key, because the transport key already provides the secure communication between the service provider and the device. Thus, there is no need to send other keys for secure communications.

For at least these reasons, the rejection of claim 27 should be reversed.

B. The rejection of claims 1-15 and 28-30 under 35 U.S.C. §103(a) as being unpatentable over Mihm in view of Fujita should be reversed for failure to teach or suggest all the claimed features.

The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007):

“Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.” Quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1966).

According to the Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in view of *KSR International Co. v. Teleflex Inc.*, Federal Register, Vol. 72, No. 195, 57526, 57529 (October 10, 2007), once the *Graham* factual inquiries are resolved, there must be a

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

determination of whether the claimed invention would have been obvious to one of ordinary skill in the art based on any one of the following proper rationales:

(A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) "Obvious to try"—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007).

Furthermore, as set forth in *KSR International Co. v. Teleflex Inc.*, quoting from *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006), "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasonings with some rational underpinning to support the legal conclusion of obviousness."

Furthermore, as set forth in MPEP 2143.03, to ascertain the differences between the prior art and the claims at issue, "[a]ll claim limitations must be considered" because "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385.

If the above-identified criteria and rationales are not met, then the cited references fail to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the cited references.

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

Independent claim 1 recites, "A removable storage device suitable for use with a host comprising: a non-volatile memory configured to store a master encryption key"

The Final Office Action, on page 5, asserts these features are disclosed in paragraph 34 of Mihm, which discloses storing the EUID 162 in NV memory 160 in the device 100. However, as described above, paragraph 59 of Mihm discloses that only the service provider controls the master key, and that the master key is never transmitted. Thus, the device 100 of Mihm, including the RAM 140, ROM 150 and NV memory 160, do not store the master key. Also, Mihm fails to teach or suggest the service provider includes a removable storage device including a non-volatile memory storing a master key. Furthermore, it would not have been obvious to store the master key of Mihm in a removable storage device at the service provider, because it would allow the master key to be easily removed and copied, which is contrary to the security requirements disclosed in paragraph 59 of Mihm.

Claim 1 also recites, "a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys." For the reasons described with respect to claim 27, Mihm fails to teach or suggest encryption keys which have been encrypted using a master encryption key. Fujita was cited to teach the claimed magnetic memory. Fujita does not remedy the aforementioned deficient teachings of Mihm.

Independent claim 28 recites, "decrypting each one of the encryption keys using the master encryption key." Mihm in view of Fujita fails to teach or suggest encrypting multiple keys using a master key for the reasons stated above. Mihm in view of Fujita also fail to teach or

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

suggest encrypting multiple keys using a master key, since keys are not encrypted with a master key in Mihm in view of Fujita.

Dependent claim 30 recites, "encrypting data using the encryption keys." As described above, Mihm discloses encrypting software for secure transmission using a single transport key. However, Mihm in view of Fujita fails to teach or suggest encrypting data using multiple encryption keys. Also, Mihm in view of Fujita fails to teach or suggest encrypting data using multiple encryption keys, wherein the multiple encryption keys are encrypted using a master key.

For at least these reasons the rejection of claims 1-15 and 28-30 should be reversed.

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

(8) Conclusion


For at least the reasons given above, the rejection of claims 1-15 and 27-30 described above should be reversed and these claims allowed.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: January 13, 2009

By


Ashok K. Mannava
Registration No.: 45,301

MANNAVA & KANG, P.C.
11240 Waples Mill Road
Suite 300
Fairfax, VA 22030
(703) 652-3822
(703) 865-5150 (facsimile)

PATENT

Atty Docket No.: 10013891-1
App. Ser. No.: 10/689,157

(9) Claim Appendix

1. (Original) A removable information storage device suitable for use with a host, comprising:

a non-volatile memory configured to store a master encryption key; and

a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys.

2. (Original) The information storage device of claim 1, further comprising an encryption and decryption engine configured to encrypt and decrypt the encryption keys using the master encryption key and to encrypt and decrypt the data using one or more of the encryption keys.

3. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a magnetic memory.

4. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a read-only memory which includes fuse elements.

5. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a nitrided read-only memory.

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

6. (Original) The information storage device of claim 1, wherein the first non-volatile memory is an erasable programmable read-only memory.

7. (Original) The information storage device of claim 1, wherein the first non-volatile memory is an electronically erasable programmable read-only memory.

8. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a flash erasable programmable read-only memory.

9. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a one time programmable read-only memory.

10. (Original) The information storage device of claim 1, wherein the non-volatile magnetic memory is a magnetic random access memory.

11. (Original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas.

12. (Original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys and

PATENT

Atty Docket No.: 10013891-1
App. Ser. No.: 10/689,157

the encrypted data are stored in the first areas.

13. (Original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the first and second areas.

14. (Original) The information storage device of claim 13, wherein the first areas are located at one or more predetermined address locations within the second non-volatile memory.

15. (Original) The information storage device of claim 13, wherein the first areas are located at one or more random address locations within the second non-volatile memory.

16. (Withdrawn) A portable memory card, comprising:
a non-volatile memory storage device configured to store one or more encrypted encryption keys and encrypted data; and
a card controller system coupled to the memory storage device configured to store and retrieve the encrypted encryption keys and the encrypted data from the memory storage device, wherein the encryption keys are encrypted and decrypted using a master encryption key and the data is encrypted and decrypted using the encryption keys.

17. (Withdrawn) The portable memory card of claim 16, wherein the non-volatile

PATENT

Atty Docket No.: 10013891-1
App. Ser. No.: 10/689,157

memory is a magnetic memory.

18. (Withdrawn) The portable memory card of claim 16, wherein the non-volatile memory is an atomic resolution storage memory.

19. (Withdrawn) The portable memory card of claim 16, wherein the card controller system includes a non-volatile master key memory configured to store the master encryption key.

20. (Withdrawn) The portable memory card of claim 16, wherein the card controller system includes an encryption and decryption engine configured to store one or more encryption algorithms and use the encryption algorithms to encrypt and decrypt the encryption keys using the master encryption key and encrypt and decrypt the data using the encryption keys.

21. (Withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas.

22. (Withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys and the encrypted data are stored in the first areas.

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

23. (Withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the first and second areas.

24. (Withdrawn) A memory card, comprising:

- a non-volatile master key memory configured to store a master encryption key;
- an encryption and decryption engine configured to implement one or more symmetrical encryption key algorithms based on the master encryption key and encryption keys;
- a memory storage device comprising an atomic resolution storage device including a field emitter, a media and a micromover, the atomic resolution storage device configured to store the encryption keys after the encryption keys are encrypted using the master encryption key and to store data after the data is encrypted using the encryption keys;
- a host interface configured to provide a communication interface to a host;
- a memory interface configured to provide a communication interface to the memory storage device;
- a data path manager configured to manage communication of the data and the encrypted data between the host and the memory storage device; and
- a controller processor configured to control the encryption and decryption of the encryption keys using the master encryption key and the encryption and decryption of the data using the encryption keys.

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

25. (Withdrawn) An information storage device, comprising:
a non-volatile memory storage device configured to store one or more encrypted encryption keys and encrypted data;
and controller means configured to store and retrieve the encrypted encryption keys and the encrypted data from the memory storage device and to encrypt and decrypt the encryption keys using a master encryption key and to encrypt and decrypt the data using the encryption keys.

26. (Withdrawn) The information storage device of claim 25, wherein the controller means includes a non-volatile master key memory configured to store the master encryption key.

27. (Original) A method of encrypting encryption keys using a master encryption key in an information storage device, comprising:

providing the encryption keys to the information storage device;
reading a master encryption key from a non-volatile memory;
encrypting each one of the encryption keys using the master encryption key; and
writing the encrypted encryption keys to a random access memory.

28. (Original) A method of decrypting encryption keys in an information storage device, comprising:

PATENT

Atty Docket No.: 10013891-1

App. Ser. No.: 10/689,157

reading the encrypted encryption keys from a magnetic random access memory;
reading a master encryption key from a first non-volatile memory; and
decrypting each one of the encryption keys using the master encryption key.

29. (Original) The method of claim 28, comprising:

reading encrypted data from the magnetic random access memory; and
decrypting the encrypted data using the encryption keys.

30. (Original) The method of claim 28, comprising:

encrypting data using the encryption keys; and
writing the encrypted data to the magnetic random access memory.

PATENT

Atty Docket No.: 10013891-1
App. Ser. No.: 10/689,157

(10) Evidence Appendix

None.

PATENT

Atty Docket No.: 10013891-1
App. Ser. No.: 10/689,157

(11) Related Proceedings Appendix

None.